ID: 321627
Sample Name: Mozi.m
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 13:42:21
Date: 23/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report Mozi.m

Overview

General Information

Sample Name:	Mozi.m
Analysis ID:	321627
MD5:	a73ddd6ec22462..
SHA1:	ac6962542a4b23..
SHA256:	b5cf68c7cb5bb2d..

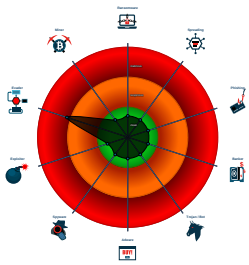
Detection

Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Creates hidden files and/or directories
- Executes the "grep" command used…
- Executes the "mkdir" command use…
- Executes the "mktemp" command u…
- Executes the "rm" command used to…
- Executes the "sleep" command use…
- Sample contains only a LOAD segm…
- Uses the "uname" system call to qu…
- Yara signature match

Classification



Startup

- **system is lnxubuntu1**
- dash New Fork (PID: 3191, Parent: 3190)
  - sed (PID: 3191, Parent: 3190, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3192, Parent: 3190)
  - sort (PID: 3192, Parent: 3190, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3193, Parent: 2523)
  - sleep (PID: 3193, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3219, Parent: 3218)
  - sed (PID: 3219, Parent: 3218, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3220, Parent: 3218)
  - sort (PID: 3220, Parent: 3218, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3222, Parent: 2523)
  - sleep (PID: 3222, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3247, Parent: 3246)
  - sed (PID: 3247, Parent: 3246, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3248, Parent: 3246)
  - sort (PID: 3248, Parent: 3246, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3249, Parent: 2523)
  - sleep (PID: 3249, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3275, Parent: 3274)
  - sed (PID: 3275, Parent: 3274, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3276, Parent: 3274)
  - sort (PID: 3276, Parent: 3274, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3277, Parent: 2523)
  - sleep (PID: 3277, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3303, Parent: 3302)
  - sed (PID: 3303, Parent: 3302, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3304, Parent: 3302)
  - sort (PID: 3304, Parent: 3302, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3310, Parent: 2523)
  - sleep (PID: 3310, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3331, Parent: 3330)
  - sed (PID: 3331, Parent: 3330, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3332, Parent: 3330)
  - sort (PID: 3332, Parent: 3330, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3333, Parent: 2523)
  - sleep (PID: 3333, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3359, Parent: 3358)
  - sed (PID: 3359, Parent: 3358, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3360, Parent: 3358)
  - sort (PID: 3360, Parent: 3358, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3361, Parent: 2523)
  - sleep (PID: 3361, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3387, Parent: 3386)
  - sed (PID: 3387, Parent: 3386, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3388, Parent: 3386)
  - sort (PID: 3388, Parent: 3386, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3403, Parent: 2523)
  - sleep (PID: 3403, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1

- dash New Fork (PID: 3415, Parent: 3414)
  - sed (PID: 3415, Parent: 3414, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3416, Parent: 3414)
  - sort (PID: 3416, Parent: 3414, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3429, Parent: 2523)
  - sleep (PID: 3429, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3443, Parent: 3442)
  - sed (PID: 3443, Parent: 3442, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3444, Parent: 3442)
  - sort (PID: 3444, Parent: 3442, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3445, Parent: 2523)
  - sleep (PID: 3445, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
  - Mozi.m (PID: 3475, Parent: 3133, MD5: a73ddd6ec22462db955439f665cad4e6) Arguments: /usr/bin/qemu-mips /tmp/Mozi.m
- upstart New Fork (PID: 3491, Parent: 2015)
  - sh (PID: 3491, Parent: 2015, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 3492, Parent: 3491)
    - date (PID: 3492, Parent: 3491, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 3493, Parent: 3491)
    - apport-checkreports (PID: 3493, Parent: 3491, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
- upstart New Fork (PID: 3518, Parent: 2015)
  - sh (PID: 3518, Parent: 2015, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 3519, Parent: 3518)
    - date (PID: 3519, Parent: 3518, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 3520, Parent: 3518)
    - apport-gtk (PID: 3520, Parent: 3518, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- dash New Fork (PID: 3546, Parent: 3545)
  - sed (PID: 3546, Parent: 3545, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3547, Parent: 3545)
  - sort (PID: 3547, Parent: 3545, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3556, Parent: 2523)
  - sleep (PID: 3556, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- upstart New Fork (PID: 3573, Parent: 2015)
  - sh (PID: 3573, Parent: 2015, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 3574, Parent: 3573)
    - date (PID: 3574, Parent: 3573, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 3583, Parent: 3573)
    - apport-gtk (PID: 3583, Parent: 3573, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- dash New Fork (PID: 3601, Parent: 3600)
  - sed (PID: 3601, Parent: 3600, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3602, Parent: 3600)
  - sort (PID: 3602, Parent: 3600, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3614, Parent: 2523)
  - sleep (PID: 3614, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3629, Parent: 3628)
  - sed (PID: 3629, Parent: 3628, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3630, Parent: 3628)
  - sort (PID: 3630, Parent: 3628, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3642, Parent: 2523)
  - sleep (PID: 3642, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3657, Parent: 3656)
  - sed (PID: 3657, Parent: 3656, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
- dash New Fork (PID: 3658, Parent: 3656)
  - sort (PID: 3658, Parent: 3656, MD5: fb4c334af5810c835b37ec2ec14a35bd) Arguments: sort -u
- dash New Fork (PID: 3669, Parent: 2523)
  - sleep (PID: 3669, Parent: 2523, MD5: e9887f1d8cae3dc50b4cbac09435a162) Arguments: sleep 1
- dash New Fork (PID: 3684, Parent: 2523)
  - sed (PID: 3684, Parent: 2523, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -n "/^DOMAINS=/ { s/^.*=/search /; p}" /run/systemd/netif/state
- dash New Fork (PID: 3685, Parent: 2523)
  - resolvconf (PID: 3685, Parent: 2523, MD5: 4e4ff2bfda7a6d18405a462937b63a2e) Arguments: /bin/sh /sbin/resolvconf -a networkd
    - resolvconf New Fork (PID: 3686, Parent: 3685)
    - mkdir (PID: 3686, Parent: 3685, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /run/resolvconf/interface
    - resolvconf New Fork (PID: 3687, Parent: 3685)
      - resolvconf New Fork (PID: 3688, Parent: 3687)
      - sed (PID: 3688, Parent: 3687, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -e s/#.*$// -e s/[[:blank:]]\\+$// -e s/^[[:blank:]]\\+// -e "s/[[:blank:]]\\+/ /g" -e "/^nameserver/!b ENDOFCYCLE" -e "s/$/ /" -e "s/\\([:.]\\)0\\+/\\10/g" -e "s/\\([:.]\\)0\\([123456789abcdefABCDEF][[:xdigit:]]*\\)/\\1\\2/g" -e "/::/b ENDOFCYCLE; s/ \\(0[:]\\)\\+/ ::/" -e "/::/b ENDOFCYCLE; s/:\\(0[:]\\)\\+/::/" -e ": ENDOFCYCLE" -
      - resolvconf New Fork (PID: 3689, Parent: 3687)
      - sed (PID: 3689, Parent: 3687, MD5: c1a00c583ba08e728b10f3f46f5776d6) Arguments: sed -e s/[[:blank:]]\\+$// -e /^$/d
- dash New Fork (PID: 3735, Parent: 2079)
  - mkdir (PID: 3735, Parent: 2079, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /home/user/.cache/logrotate
- dash New Fork (PID: 3736, Parent: 2079)
  - mkdir (PID: 3736, Parent: 2079, MD5: a97f666f21c85ec62ea47d022263ef41) Arguments: mkdir -p /home/user/.cache/upstart
- dash New Fork (PID: 3737, Parent: 2079)
  - egrep (PID: 3737, Parent: 2079, MD5: unknown) Arguments: /bin/sh /bin/egrep [^[:print:]] /home/user/.cache/logrotate/status
  - grep (PID: 3737, Parent: 2079, MD5: fc9b0a0ff848b35b3716768695bf2427) Arguments: grep -E [^[:print:]] /home/user/.cache/logrotate/status
- dash New Fork (PID: 3738, Parent: 2079)
  - mktemp (PID: 3738, Parent: 2079, MD5: 91cf2e2a84f3b49fdecdd8b631902009) Arguments: mktemp
- dash New Fork (PID: 3791, Parent: 2079)
  - cat (PID: 3791, Parent: 2079, MD5: efa10d52f37361f2e3a5d22742f0fcc4) Arguments: cat
- dash New Fork (PID: 3816, Parent: 2079)
  - logrotate (PID: 3816, Parent: 2079, MD5: d0eaf9942936032d217478b93e9cd4b1) Arguments: logrotate -s /home/user/.cache/logrotate/status /tmp/tmp.KSLFY1dTfT
    - logrotate New Fork (PID: 3825, Parent: 3816)
    - gzip (PID: 3825, Parent: 3816, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3826, Parent: 3816)
    - gzip (PID: 3826, Parent: 3816, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3827, Parent: 3816)
    - gzip (PID: 3827, Parent: 3816, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3828, Parent: 3816)
    - gzip (PID: 3828, Parent: 3816, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
    - logrotate New Fork (PID: 3829, Parent: 3816)

- logrotate New Fork (PID: 3830, Parent: 3816)
  - gzip (PID: 3830, Parent: 3816, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
  - logrotate New Fork (PID: 3835, Parent: 3816)
  - gzip (PID: 3835, Parent: 3816, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
  - logrotate New Fork (PID: 3843, Parent: 3816)
  - gzip (PID: 3843, Parent: 3816, MD5: 25ea567880cec4ac02e7a77ad304e3c6) Arguments: /bin/gzip
- dash New Fork (PID: 3875, Parent: 2079)
  - rm (PID: 3875, Parent: 2079, MD5: b79876063d894c449856cca508ecca7f) Arguments: rm -f /tmp/tmp.KSLFY1dTfT
  - **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Mozi.m	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x206f8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x20767:$s2: $Id: UPX • 0x20718:$s3: $Info: This file is packed with the UPX executable packer

Signature Overview

Click to jump to signature section

- AV Detection
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Malware Analysis System Evasion

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Data Obfuscation:

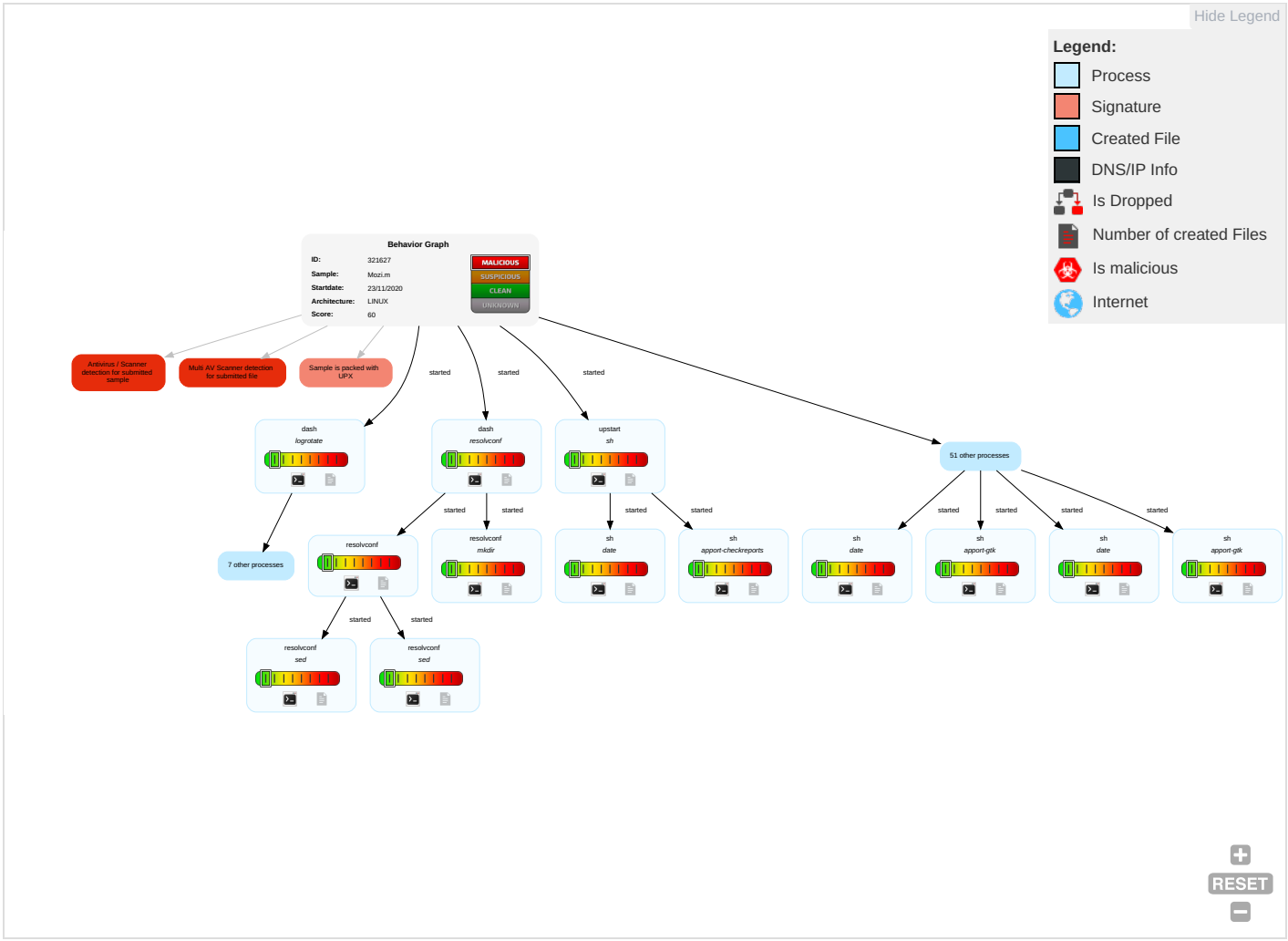
Sample is packed with UPX

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Hidden Files and Directories 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modi Syst Parti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devi Lock

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	File Deletion 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Dele Devi Data

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Mozi.m	18%	Metadefender		Browse
Mozi.m	59%	ReversingLabs	Linux.Trojan.Mirai	
Mozi.m	100%	Avira	LINUX/Mirai.ccjqy	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321627
Start date:	23.11.2020
Start time:	13:42:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Mozi.m
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 16.04 x64 (Kernel 4.4.0-116, Firefox 59.0, Document Viewer 3.18.2, LibreOffice 5.1.6.2, OpenJDK 1.8.0_171)
Detection:	MAL
Classification:	mal60.evad.linM@0/11@0/0
Warnings:	Show All

Runtime Messages

Command:	/tmp/Mozi.m
Exit Code:	133
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	qemu: uncaught target signal 5 (Trace/breakpoint trap) - core dumped

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/home/user/.cache/logrotate/status.tmp	
Process:	/usr/sbin/logrotate
File Type:	ASCII text
Category:	dropped
Size (bytes):	1451
Entropy (8bit):	4.863962167704535
Encrypted:	false
SSDEEP:	24:fOeWfnS8MHqIJWfnrQHLWfnw7WfnDv0TGMHmIbCMHtW8MF8iQlGwWfnRvCMHs:2elNHqcsAnRHmoHtWbFLWsDHs
MD5:	E48DC5B941150D0C9EFF284325CFFA6B
SHA1:	6DA961B9B4D67AFEB0C8BA3A932C4C0754CFBC58
SHA-256:	00132B083560E3DD1352853BC714A64D054AD9F65EB3F301DF104B420D5EFD5E
SHA-512:	C1050E8420468B1323E32A854F377F61C16A55D706A8BBB5D14AD9CC184549E640FFC24F93D02F92803646D2286C6AD47597954EBE801DF440E73AE281A5998C
Malicious:	false
Reputation:	low
Preview:	logrotate state -- version 2."/home/user/.cache/upstart/indicator-application.log" 2018-5-7-11:38:22."/home/user/.cache/upstart/indicator-sound.log" 2018-5-7-10:33:19."/home/user/.cache/upstart/update-notifier-crash-_var_crash__usr_share_apport_apport-gtk.1000.crash.log" 2020-11-23-14:0:0."/home/user/.cache/upstart/indicator-session.log" 2018-5-7-11:38:22."/home/user/.cache/upstart/dbus.log" 2020-11-23-14:43:7."/home/user/.cache/upstart/gnome-keyring-ssh.log" 2020-11-23-14:43:7."/home/user/.cache/upstart/indicator-bluetooth.log" 2018-5-7-11:38:22."/home/user/.cache/upstart/indicator-datetime.log" 2018-5-7-11:38:22."/home/user/.cache/upstart/startxfce4.log" 2020-11-23-14:43:7."/home/user/.cache/upstart/update-notifier-release.log" 2020-11-23-14:43:7."/home/user/.cache/upstart/update-notifier-crash-_var_crash__usr_share_apport_apport.0.crash.log" 2020-11-23-14:0:0."/home/user/.cache/upstart/ssh-agent.log" 2020-11-23-14:43:7."/home/user/.cache/upstart/update-notifier-crash-_var_crash__usr

/home/user/.cache/upstart/dbus.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Nov 23 12:42:26 2020, from Unix
Category:	dropped
Size (bytes):	267
Entropy (8bit):	7.175239390630417
Encrypted:	false
SSDEEP:	6:XZnYlQuom0gW0F46ASWpC8t0BEP80ryEbjL+swraiuWRGI:X5/nLT0F48WUTBEEAJPyROi0I
MD5:	D7444F7D824BD0C899CA8FD73786D0C6
SHA1:	F3D578A1A7E9119455799B4FE53DC5FB54D0AEE9
SHA-256:	F70398771CEF85ADEABBEF2A75062CD90EB08EAAC4FE8E8D6AD53FBAB5EB917A
SHA-512:	5C6440511A148026E28843AC963800C52D7CF42A10E45256B08BA4262F26CD675DFA413D237AB2DE87C28EE3BFF91A3421FF444D110BF1691C00FF1579AAE50A
Malicious:	false
Reputation:	low
Preview:	....2.._.....N.0...H.Co.E*w.E.8.MbL....EMc.;...3....._~..?....i....=./(...,.....9[....p,.....!..p..ANb.e..0....(.y...K...N..<.x..i."+.j=.tfpl..=Ee...."....|`..zb*..KKQ.|Yz..nK!....."'T..f=G=.....s.#.N...eOD....s...u....h@..+...j...P.....A.S.....

/home/user/.cache/upstart/gnome-keyring-ssh.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Jul 27 09:05:22 2020, from Unix
Category:	dropped
Size (bytes):	99
Entropy (8bit):	6.129257882662173
Encrypted:	false
SSDEEP:	3:FtPaGuofByOJ9+JbgcpuvfIMGddoffEwZW/l:XPa25NrQbgYuoMBfMsGl
MD5:	2B8D9549C00943FB9FFC73FD80E6AC1A
SHA1:	E6348E8BB25396F0542E7E74AE30AF03F48E237E

/home/user/.cache/upstart/gnome-keyring-ssh.log.1.gz	
SHA-256:	606AE477FACBE88A7BF8C1718AE0259E50487BB5F98B80F0E2895DD799BBE858
SHA-512:	C2CA8D2DFC0B0E28FDB3E94EF2BE74D7D663E9943EE55D03F9F8C8E1425AC4C0C07391020DEE0931EC9967185BDD75BDA438BC413DDBC6AB18D2EF28388C D59
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....._..... ....;t...!.@....-.....+B..X.%.J.>..`..jA....:-i.8...i7..f..+....@jB.X.y.OK..Y...

/home/user/.cache/upstart/gpg-agent.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Jul 27 09:05:26 2020, from Unix
Category:	dropped
Size (bytes):	109
Entropy (8bit):	6.285347714840308
Encrypted:	false
SSDEEP:	3:Ft+KspyDBmKyr7JtqZioTFBkdMl/:X+KspyDB94JtYPk+
MD5:	13A3054AF030A536BDA784F022481B4C
SHA1:	062CEC7C61E642887CE10970A7353066C4283DFD
SHA-256:	0D9475D2511F0A2C555242326C2D4EB69E4456726BDDB84913B95EC59F8FDCF6
SHA-512:	EB0A9DDC9D084934F42DF3AC9FE92CE534A841B38F6008774F29788EEFEC4FD22BFE12570B30558A351755347E92742C867B3B65E0616294146C390FB60A3388
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....._.....0....=l...E.C....p&.....fX.L..Wt...)*.*...e.X.....).Fj+.,."E..5f.....X.K..w.....

/home/user/.cache/upstart/ssh-agent.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Jul 27 09:05:22 2020, from Unix
Category:	dropped
Size (bytes):	60
Entropy (8bit):	5.121567004295788
Encrypted:	false
SSDEEP:	3:FtPa5qBO0YYLB0trl1mlwdn:XPa5W2Yt02g6n
MD5:	32CF70DC61DECD8DFBC64EB2F2529FAC
SHA1:	DAC70D15E4E11407299DC63AAA6774A2393C2316
SHA-256:	5F46EF0AAB4AD28F5384537011EDB096F22592BE4EA83194C1A52A11ECAD51D5
SHA-512:	D89B691D4403CB3B836F4B50795046DE26AC588D2C03020EC9B944B97259DD7ED759509229E92B601C5050F2A43DCAFA0D098E2EE5E324A56F69E1EE4BB35E8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....._..+...MLO.+Q(.././(J.-.I,*.Q((.ON-.V024.....["(...

/home/user/.cache/upstart/startxfce4.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Nov 23 13:42:50 2020, from Unix
Category:	dropped
Size (bytes):	1151
Entropy (8bit):	7.841487373623072
Encrypted:	false
SSDEEP:	24:X7d+BojMnJnBU5Lk9eIEtZHE9LYIOzgczACtLQ1vzKpDk/aR:X7d+iI9u5LCEtFE9LBOzjACEKQA
MD5:	B6571D514861C61D0964A3BEFEBC3135
SHA1:	947736E5F427E7E1CFA72E543588E382F9D2384C
SHA-256:	3CC31B2F656CEC1432138ADA16B859EBEC70A34F6BF040EE94EED2CC3CD7C848
SHA-512:	3CD6D4E0FFDAAE30EBE6116BF47E4556E7794CE6DD0B01A733BC195E832E4A98C074AD8DB6E99C03F6BE94C2082C29142496878C81F2EC1658146BE82FC115 0
Malicious:	false
Reputation:	low
Preview:	....Z.._...V.n.8....?....d;.M.t#....i'...@Ke..D...V.~....9...s. ..W.{E...7.u}..?.~:J...<.3...w..t...)L..`.....R..z.T.fi...g....%7...s.....1\...`%.....T.._.e.Ln.}.0.....y.@K...$us...;A..jH..`.gt2." 1.i..I\_.X....h'....(.Q.k.....oW..Z1.g...n...U.....B..-.....k.$..t.K.v.`.c...~..nKU&.,"J]X..:.-.n.#j..uoq.....Y%Y.=G.O..w...?.]@..U...$.Y....7..7s.....u:8.K.....pc..-.g)c..KH@.j.m...9 ._X.S..4...).O.-.k>...&.....N....L.L.:3.W5.f(^...v.~.....}.3bE.O.....5.....<.4y..4.{..3q.R*u..5b'..e+.'.....R.5... X.[..%...}k..kf@H.J../...!r5...*P..$...p..R..a<HG..w..n.$..r.....f,_V.\. x:g.N$f.4.?p3"y.y.).....m....]...x.i..1....3...^.Z....6}.....\...A(y..#.g..a...@.....Rc.....8Z..f..tHf.^"%.....(i...[..Q....6.t4.....+"..l.E!..9..$..V.S..h.H..F....BF..Q..d.y.<a..H.../..U.I .]0.9.h...c.J.;....p;.<.I6k....Y.:...9..>.....^...w.4..e..K..u...i.DPIg.....rP.....;....>..).(.+*.....E.p..W$....<;..vE\P..*.I.^S....e.>.1|.v.K...EK.B....;...uZPG.8.:J.&.....@

/home/user/.cache/upstart/update-notifier-release.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Jul 27 09:05:22 2020, from Unix

/home/user/.cache/upstart/update-notifier-release.log.1.gz	
Category:	dropped
Size (bytes):	73
Entropy (8bit):	5.311208593298957
Encrypted:	false
SSDEEP:	3:FtPacK82rsFX+TP4P2gt:XPacf2rNWt
MD5:	6B9C8B79E6508C02BCACF1C11363D3BC
SHA1:	F450E69D5A258FCF4D89E7CDB1FBD7EEC5E19A77
SHA-256:	735DFDFE533A05589BFDC9044627395F29312064CFBA09CCB60E010AEC692411
SHA-512:	AAE4EF554245D1419335B80EA6ED0E357FCC7032BF991D4808B8A2E09F671BA318B7EF0A8824FA334D6B51EF7104351461814D1EE096D357305914A83380CC35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......_.....S.*.Q02W04.20.22Rpv..Q0202P.K-W(J.IM,NUH,K..IL.I.....5...

/home/user/.cache/upstart/upstart-event-bridge.log.1.gz	
Process:	/bin/gzip
File Type:	Mon Jul 27 09:05:22 2020, from Unix
Category:	dropped
Size (bytes):	68
Entropy (8bit):	5.395998870534845
Encrypted:	false
SSDEEP:	3:FtPa5wG0BMPWNLPgXseOBMky:XPa5wG+OQP4OBMV
MD5:	1395D405968C76307CBA75C5DDC9CA19
SHA1:	C36CEE03E5DF12FBFB57A5EBCEAE329B41AFA1F7
SHA-256:	33785027CEE82E878434593B532FE1DF25D46676379757272C1E15C9AADD3B1F
SHA-512:	09CAB8DFF495DA9ED715C94E9F24B0C5C40CF0BC8C1B0DEEFB90C54081020AD80AF51636ADCBA368980E2C69119697A65E2E4AC5B834E0F08F88AEA52EFDA57
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......_..+-(.I,*.M-K.+.M*.LIOU(../.(J....(...'...+..X..r.....3...

/tmp/tmp.KSLFY1dTfT	
Process:	/bin/cat
File Type:	ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	3.7760909131289533
Encrypted:	false
SSDEEP:	3:PgWA0uU95y/1aF/g2FFXwyyVDoGeRqcOAvC:PgWl195y9aF/g2FFgfNepvK
MD5:	46261223A62EF65D03C70F15EE935267
SHA1:	E9102D8808BA6E171405F1830BD7C6B8179C9BF2
SHA-256:	DFECC8990014230F50FBAD269AD523A74D16CFB455065EC8D9041764D684C239
SHA-512:	380CFA479D6DB2361DCE6A52A516ECBA4D5CCE647299A87C3C3ED5887DB929C81A0F970097E6CF02C11440BCE87299D611B01CE56CF9AF09DCFBBA14249E9F9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	"/home/user/.cache/upstart/*.log" {. hourly. missingok. rotate 7. compress. notifempty. nocreate.}.

/var/crash/_usr_share_apport_apport-checkreports.1000.crash	
Process:	/usr/share/apport/apport-checkreports
File Type:	ASCII text
Category:	dropped
Size (bytes):	14915
Entropy (8bit):	4.693135471731997
Encrypted:	false
SSDEEP:	384:C5c5QaaB/aGl047vasNDydz/30UuTEE/LL:CvTE2
MD5:	2ED5FD8C8E5EBF3E7CB8798F8E394A1A
SHA1:	C2EB9EC1CF5CD9A7B6CEEE6F866F8EDBF358E235
SHA-256:	F0E4E855B49B60D86C6E4CEF0E1E8ECA88BAF5D4631B2D3F19BE7F043E7BE9FD
SHA-512:	698732A11628A54F72304FC1C944271FE6C1A7B82558C176224F3847424E4843E945D7F13000283887F2FA37BE6DF6EBDBAA1E1906763D57418A2B200F41D162
Malicious:	false
Reputation:	low

/var/crash/_usr_share_apport_apport-checkreports.1000.crash	
Preview:	ProblemType: Crash.Date: Mon Nov 23 14:42:51 2020.ExecutablePath: /usr/share/apport/apport-checkreports.ExecutableTimestamp: 1514927430.InterpreterPath: /usr/bin/python3.5.ProcCmdline: /usr/bin/python3 /usr/share/apport/apport-checkreports --system.ProcCwd: /home/user.ProcEnviron:. LANGUAGE=en_US. PATH=(custom, user). XDG_RUNTIME_DIR=<set>. LANG=en_US.UTF-8. SHELL=/bin/bash.ProcMaps:. 00400000-007a9000 r-xp 00000000 fc:00 217 /usr/bin/python3.5. 009a9000-009ab000 r--p 003a9000 fc:00 217 /usr/bin/python3.5. 009ab000-00a42000 rw-p 003ab000 fc:00 217 /usr/bin/python3.5. 00a42000-00a73000 rw-p 00000000 00:00 0 . 01d8d000-020e6000 rw-p 00000000 00:00 0 [heap]. 7fab42afe000-7fab42c7f000 rw-p 00000000 00:00 0 . 7fab42c7f000-7fab42c96000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7fab42c96000-7fab42e95000 ---p 00017000 fc:0

/var/crash/_usr_share_apport_apport-gtk.1000.crash	
Process:	/usr/share/apport/apport-gtk
File Type:	ASCII text
Category:	dropped
Size (bytes):	47094
Entropy (8bit):	4.501454079173753
Encrypted:	false
SSDEEP:	768:DllTO/f/Z/p/FzaHofEOGc1OH/8lyKkUoe:DlU/f/Z/p/AOGc1OH/8lyKkY
MD5:	1EF798E410D462921025A6AB3F2892B3
SHA1:	52071794564CDE472767C241D5ED90C3D64FE4B0
SHA-256:	F367DEEFBEA1919924004E3CA43C3B1BC1E42B5E39208D98A67A2D6DE04CFA06
SHA-512:	6788E793B81065530E1138DF44A6DAE1B8F2CEA27A64E604CF01A4EA388C5C4C2D9CC321A72C629D6CAB19C7FC5A6157CA0D9FEC5A29C27C63319E16EA3567
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Mon Nov 23 14:42:51 2020.ExecutablePath: /usr/share/apport/apport-gtk.ExecutableTimestamp: 1514927430.InterpreterPath: /usr/bin/python3.5.ProcCmdline: /usr/bin/python3 /usr/share/apport/apport-gtk.ProcCwd: /home/user.ProcEnviron:. LANGUAGE=en_US. PATH=(custom, user). XDG_RUNTIME_DIR=<set>. LANG=en_US.UTF-8. SHELL=/bin/bash.ProcMaps:. 00400000-007a9000 r-xp 00000000 fc:00 217 /usr/bin/python3.5. 009a9000-009ab000 r--p 003a9000 fc:00 217 /usr/bin/python3.5. 009ab000-00a42000 rw-p 003ab000 fc:00 217 /usr/bin/python3.5. 00a42000-00a73000 rw-p 00000000 00:00 0 . 01ac5000-01fe6000 rw-p 00000000 00:00 0 [heap]. 7fb679e71000-7fb679f71000 rw-p 00000000 00:00 0 . 7fb679f71000-7fb679f88000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7fb679f88000-7fb67a187000 ---p 00017000 fc:00 2382

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.813637944981102
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	Mozi.m
File size:	135472
MD5:	a73ddd6ec22462db955439f665cad4e6
SHA1:	ac6962542a4b23ac13bddff22f8df9aeb702ef12
SHA256:	b5cf68c7cb5bb2d21d60bf6654926f61566d95bfd7c9f9e182d032f1da5b4605
SHA512:	92a52f68a7324c4d5876e1f7e2cb87d14b8604b057ceee2e537815568faa96abf576a22111c5c976eff72ab9015f1261b2331d4b4d711f4e62c8eb403c2377aa
SSDEEP:	3072:2glZ3FtCKXhkmHtZ9TEKzjfj/WMngyIfsJ0F7xPtoM:2IIKXhZtL7jOTyIG87Xl
File Content Preview:	.ELF.....B.x...4.....4. ...(.....@...@.....C...C.....*.*UPX!.X.....]....|.$..ELF.....@.`....4...p... ...(.....<...@.....[v.....H...`.t/._...dt.Q.....].M.....P.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V

ELF header	
ABI Version:	0
Entry Point Address:	0x420578
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x20fc2	0x20fc2	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x91f18	0x6	RW	0x10000		

Network Behavior

No network behavior found

System Behavior

Analysis Process: dash PID: 3191 Parent PID: 3190

General

Start time:	13:42:41
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3191 Parent PID: 3190

General

Start time:	13:42:41
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3192 Parent PID: 3190

General

Start time:	13:42:41
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3192 Parent PID: 3190

General

Start time:	13:42:41
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3193 Parent PID: 2523

General

Start time:	13:42:41
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3193 Parent PID: 2523

General

Start time:	13:42:41
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3219 Parent PID: 3218

General

Start time:	13:42:42

Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3219 Parent PID: 3218

General

Start time:	13:42:42
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3220 Parent PID: 3218

General

Start time:	13:42:42
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3220 Parent PID: 3218

General

Start time:	13:42:42
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3222 Parent PID: 2523

General

Start time:	13:42:42
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a

File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3222 Parent PID: 2523

General

Start time:	13:42:42
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3247 Parent PID: 3246

General

Start time:	13:42:43
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3247 Parent PID: 3246

General

Start time:	13:42:43
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3248 Parent PID: 3246

General

Start time:	13:42:43
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3248 Parent PID: 3246

General

Start time:	13:42:43
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3249 Parent PID: 2523

General

Start time:	13:42:43
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3249 Parent PID: 2523

General

Start time:	13:42:43
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3275 Parent PID: 3274

General

Start time:	13:42:44
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3275 Parent PID: 3274

General

Start time:	13:42:44
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3276 Parent PID: 3274

General

Start time:	13:42:44
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3276 Parent PID: 3274

General

Start time:	13:42:44
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3277 Parent PID: 2523

General

Start time:	13:42:44
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3277 Parent PID: 2523

General

Start time:	13:42:44
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3303 Parent PID: 3302

General

Start time:	13:42:45
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3303 Parent PID: 3302

General

Start time:	13:42:45
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3304 Parent PID: 3302

General

Start time:	13:42:45
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3304 Parent PID: 3302

General

Start time:	13:42:45

Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3310 Parent PID: 2523

General

Start time:	13:42:45
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3310 Parent PID: 2523

General

Start time:	13:42:45
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3331 Parent PID: 3330

General

Start time:	13:42:46
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3331 Parent PID: 3330

General

Start time:	13:42:46
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*

File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3332 Parent PID: 3330

General

Start time:	13:42:46
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3332 Parent PID: 3330

General

Start time:	13:42:46
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3333 Parent PID: 2523

General

Start time:	13:42:46
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3333 Parent PID: 2523

General

Start time:	13:42:46
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3359 Parent PID: 3358

General

Start time:	13:42:47
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3359 Parent PID: 3358

General

Start time:	13:42:47
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3360 Parent PID: 3358

General

Start time:	13:42:47
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3360 Parent PID: 3358

General

Start time:	13:42:47
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3361 Parent PID: 2523

General

Start time:	13:42:47
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3361 Parent PID: 2523

General

Start time:	13:42:47
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3387 Parent PID: 3386

General

Start time:	13:42:48
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3387 Parent PID: 3386

General

Start time:	13:42:48
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3388 Parent PID: 3386

General

Start time:	13:42:48
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3388 Parent PID: 3386

General

Start time:	13:42:48
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3403 Parent PID: 2523

General

Start time:	13:42:48
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3403 Parent PID: 2523

General

Start time:	13:42:48
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3415 Parent PID: 3414

General

Start time:	13:42:49
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3415 Parent PID: 3414

General

Start time:	13:42:49
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3416 Parent PID: 3414

General

Start time:	13:42:49
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3416 Parent PID: 3414

General

Start time:	13:42:49
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3429 Parent PID: 2523

General

Start time:	13:42:49

Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3429 Parent PID: 2523

General

Start time:	13:42:49
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3443 Parent PID: 3442

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3443 Parent PID: 3442

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3444 Parent PID: 3442

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a

File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3444 Parent PID: 3442

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3445 Parent PID: 2523

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3445 Parent PID: 2523

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: Mozi.m PID: 3475 Parent PID: 3133

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/tmp/Mozi.m
Arguments:	/usr/bin/qemu-mips /tmp/Mozi.m
File size:	135472 bytes
MD5 hash:	a73ddd6ec22462db955439f665cad4e6

File Activities

File Read

Analysis Process: upstart PID: 3491 Parent PID: 2015

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 3491 Parent PID: 2015

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 3492 Parent PID: 3491

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 3492 Parent PID: 3491

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 3493 Parent PID: 3491

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 3493 Parent PID: 3491

General

Start time:	13:42:50
Start date:	23/11/2020
Path:	/usr/share/apport/apport-checkreports
Arguments:	/usr/bin/python3 /usr/share/apport/apport-checkreports --system
File size:	1269 bytes
MD5 hash:	1a7d84ebc34df04e55ca3723541f48c9

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: upstart PID: 3518 Parent PID: 2015

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 3518 Parent PID: 2015

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 3519 Parent PID: 3518

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 3519 Parent PID: 3518

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 3520 Parent PID: 3518

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 3520 Parent PID: 3518

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/usr/share/apport/apport-gtk
Arguments:	/usr/bin/python3 /usr/share/apport/apport-gtk
File size:	23806 bytes
MD5 hash:	ec58a49a30ef6a29406a204f28cc7d87

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: dash PID: 3546 Parent PID: 3545

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3546 Parent PID: 3545

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3547 Parent PID: 3545

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3547 Parent PID: 3545

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3556 Parent PID: 2523

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3556 Parent PID: 2523

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: upstart PID: 3573 Parent PID: 2015

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 3573 Parent PID: 2015

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 3574 Parent PID: 3573

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 3574 Parent PID: 3573

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 3583 Parent PID: 3573

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 3583 Parent PID: 3573

General

Start time:	13:42:51
Start date:	23/11/2020
Path:	/usr/share/apport/apport-gtk
Arguments:	/usr/bin/python3 /usr/share/apport/apport-gtk
File size:	23806 bytes
MD5 hash:	ec58a49a30ef6a29406a204f28cc7d87

File Activities

File Read

Directory Enumerated

Analysis Process: dash PID: 3601 Parent PID: 3600

General

Start time:	13:42:52
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3601 Parent PID: 3600

General

Start time:	13:42:52
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3602 Parent PID: 3600

General

Start time:	13:42:52
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3602 Parent PID: 3600

General

Start time:	13:42:52
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3614 Parent PID: 2523

General

Start time:	13:42:52
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3614 Parent PID: 2523

General

Start time:	13:42:52
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3629 Parent PID: 3628

General

Start time:	13:42:53
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3629 Parent PID: 3628

General

Start time:	13:42:53
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3630 Parent PID: 3628

General

Start time:	13:42:53

Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3630 Parent PID: 3628

General

Start time:	13:42:53
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3642 Parent PID: 2523

General

Start time:	13:42:53
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3642 Parent PID: 2523

General

Start time:	13:42:53
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3657 Parent PID: 3656

General

Start time:	13:42:54
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a

File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3657 Parent PID: 3656

General

Start time:	13:42:54
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DNS=/ { s/^DNS=/nameserver /; p}" /run/systemd/netif/state /run/systemd/netif/leases/*
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3658 Parent PID: 3656

General

Start time:	13:42:54
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sort PID: 3658 Parent PID: 3656

General

Start time:	13:42:54
Start date:	23/11/2020
Path:	/usr/bin/sort
Arguments:	sort -u
File size:	110040 bytes
MD5 hash:	fb4c334af5810c835b37ec2ec14a35bd

File Activities

File Read

Analysis Process: dash PID: 3669 Parent PID: 2523

General

Start time:	13:42:54
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sleep PID: 3669 Parent PID: 2523

General

Start time:	13:42:54
Start date:	23/11/2020
Path:	/bin/sleep
Arguments:	sleep 1
File size:	31408 bytes
MD5 hash:	e9887f1d8cae3dc50b4cbac09435a162

File Activities

File Read

Analysis Process: dash PID: 3684 Parent PID: 2523

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sed PID: 3684 Parent PID: 2523

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -n "/^DOMAINS=/ { s/^.*=/search /; p}" /run/systemd/netif/state
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3685 Parent PID: 2523

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: resolvconf PID: 3685 Parent PID: 2523

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/sbin/resolvconf
Arguments:	/bin/sh /sbin/resolvconf -a networkd
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

File Activities

File Read

Analysis Process: resolvconf PID: 3686 Parent PID: 3685

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: mkdir PID: 3686 Parent PID: 3685

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/bin/mkdir
Arguments:	mkdir -p /run/resolvconf/interface
File size:	76848 bytes
MD5 hash:	a97f666f21c85ec62ea47d022263ef41

File Activities

File Read

Directory Created

Analysis Process: resolvconf PID: 3687 Parent PID: 3685

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: resolvconf PID: 3688 Parent PID: 3687

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: sed PID: 3688 Parent PID: 3687

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -e s/#.*$// -e s/[[:blank:]]\\+$// -e s/^[[:blank:]]\\+// -e "s/[[:blank:]]\\+/ /g" -e "/^nameserver/!b ENDOFCYCLE" -e "s/$/ /" -e "s/\\([:.]\\)0\\+/\\10/g" -e "s/\\([:.]\\)0\\([123456789abcdefABCDEF][[:xdigit:]]*\\)/\\1\\2/g" -e "/::/b ENDOFCYCLE; s/ \\(0[:]\\)\\+/ ::/" -e "/::/b ENDOFCYCLE; s/:\\(0[:]\\)\\+/::/" -e ": ENDOFCYCLE" -
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: resolvconf PID: 3689 Parent PID: 3687

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/sbin/resolvconf
Arguments:	n/a
File size:	4590 bytes
MD5 hash:	4e4ff2bfda7a6d18405a462937b63a2e

Analysis Process: sed PID: 3689 Parent PID: 3687

General

Start time:	13:42:55
Start date:	23/11/2020
Path:	/bin/sed
Arguments:	sed -e s/[[:blank:]]\\+$// -e /^$/d
File size:	73424 bytes
MD5 hash:	c1a00c583ba08e728b10f3f46f5776d6

File Activities

File Read

Analysis Process: dash PID: 3735 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mkdir PID: 3735 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/mkdir
Arguments:	mkdir -p /home/user/.cache/logrotate
File size:	76848 bytes
MD5 hash:	a97f666f21c85ec62ea47d022263ef41

File Activities

File Read

Directory Created

Analysis Process: dash PID: 3736 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mkdir PID: 3736 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/mkdir
Arguments:	mkdir -p /home/user/.cache/upstart
File size:	76848 bytes
MD5 hash:	a97f666f21c85ec62ea47d022263ef41

File Activities

File Read

Directory Created

Analysis Process: dash PID: 3737 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: egrep PID: 3737 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/egrep
Arguments:	/bin/sh /bin/egrep [^[:print:]] /home/user/.cache/logrotate/status
File size:	0 bytes
MD5 hash:	unknown

File Activities

File Read

Analysis Process: grep PID: 3737 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/grep
Arguments:	grep -E [^[:print:]] /home/user/.cache/logrotate/status
File size:	211224 bytes
MD5 hash:	fc9b0a0ff848b35b3716768695bf2427

File Activities

File Read

Analysis Process: dash PID: 3738 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: mktemp PID: 3738 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/mktemp
Arguments:	mktemp
File size:	39728 bytes
MD5 hash:	91cf2e2a84f3b49fdecdd8b631902009

File Activities

File Read

Analysis Process: dash PID: 3791 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: cat PID: 3791 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/cat
Arguments:	cat
File size:	52080 bytes
MD5 hash:	efa10d52f37361f2e3a5d22742f0fcc4

File Activities

File Read

File Written

Analysis Process: dash PID: 3816 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: logrotate PID: 3816 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/usr/sbin/logrotate
Arguments:	logrotate -s /home/user/.cache/logrotate/status /tmp/tmp.KSLFY1dTfT
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

File Activities

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Permission Modified

Analysis Process: logrotate PID: 3825 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3825 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3826 Parent PID: 3816

General

Start time:	13:43:07

Start date:	23/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3826 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3827 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3827 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3828 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3828 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3830 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3830 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3835 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3835 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: logrotate PID: 3843 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/usr/sbin/logrotate
Arguments:	n/a
File size:	64624 bytes
MD5 hash:	d0eaf9942936032d217478b93e9cd4b1

Analysis Process: gzip PID: 3843 Parent PID: 3816

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/gzip
Arguments:	/bin/gzip
File size:	98240 bytes
MD5 hash:	25ea567880cec4ac02e7a77ad304e3c6

File Activities

File Read

File Written

Analysis Process: dash PID: 3875 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/dash
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: rm PID: 3875 Parent PID: 2079

General

Start time:	13:43:07
Start date:	23/11/2020
Path:	/bin/rm
Arguments:	rm -f /tmp/tmp.KSLFY1dTfT
File size:	60272 bytes
MD5 hash:	b79876063d894c449856cca508ecca7f

File Activities

File Deleted

File Read